UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/003,820	10/31/2001	Richard Paul Tarquini	10017334-1	4709

7590 05/15/2007
HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER	
COLIN, CARL G	
ART UNIT	PAPER NUMBER
2136	
MAIL DATE	DELIVERY MODE
05/15/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/003,820	**Applicant(s)** TARQUINI ET AL.
	Examiner Carl Colin	**Art Unit** 2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _08 January 2007_.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-20_ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-20_ is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.
4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .
5) □ Notice of Informal Patent Application
6) □ Other: _____.

DETAILED ACTION

1. In view of the Appeal Brief filed on 1/8/2007, PROSECUTION IS HEREBY REOPENED. A new ground of rejection is set forth below.

To avoid abandonment of the application, appellant must exercise one of the following two options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37 CFR 1.113 (if this Office action is final); or,

(2) initiate a new appeal by filing a notice of appeal under 37 CFR 41.31 followed by an appeal brief under 37 CFR 41.37. The previously paid notice of appeal fee and appeal brief fee can be applied to the new appeal. If, however, the appeal fees set forth in 37 CFR 41.20 have been increased since they were previously paid, then appellant must pay the difference between the increased fees and the amount previously paid.

A Supervisory Patent Examiner (SPE) has approved of reopening prosecution by signing below.

Response to Arguments

2. In response to communications filed on 1/8/2007, the following claims 1-20 are presented for examination.

2.1 Applicant's arguments, see pages 7-8, filed on 1/8/2007, with respect to the 112th rejection of claims 1-7 have been fully considered and are persuasive. The 112th rejection of claims 1-7 has been withdrawn.

Applicant's arguments, in the appeal brief filed on 1/8/2007 have been fully considered, but they are moot in view of a new ground of rejection.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-7 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent Publication US 2002/0078381 to **Farley et al** in view of US Patent 6,279,113 **Vaidya**.

As per claim 1: **Farley et al** discloses a node of a network for managing an intrusion protection system, the node (security management system (20) in fig.2) comprising: a memory module for storing data in machine-readable format for retrieval and execution by a central processing unit (see page 5, paragraph 64); and discloses the security management comprises program modules that may be implemented in conjunction with operating system programs and operable to execute an intrusion protection system management application (such as fusion engine) (see pages 3-4 paragraphs 45-47); **Farley et al** further discloses the fusion engine operable to receive text-file input (raw events or event log file) from an input device (event collector) the text file defining a network exploit rule and comprising at least one field (see page 8, paragraph 93 and page 6, paragraph 66); and comprising at least one field (see fig. 5B-5F) from which a determination is made as to whether an intrusion protection evaluates the network exploit rule (see page 7, paragraph 77 and page 14, paragraph 162); **Farley et al** discloses among others historical frequency value (see page 15, paragraphs 168-171), vulnerability status (page 13, paragraph 155), priority status values (page 14, paragraphs 160-161) for determining whether a network exploit rule has been evaluated and further discloses reason for changing the priority value is recorded so as one can determine why a particular event was assigned a reduced priority (see page 14, paragraph 167 and page 15, paragraphs 170-171). **Farley et al** is silent about the operating system comprising a network stack comprising a protocol driver and a media access control driver. These are well known features as disclosed in OSI model architecture. **Vaidya** in an analogous art discloses detecting intrusion attempts into system resources by monitoring for attack signatures comprising monitoring network data to determine whether data is associated with a network intrusion; extraction of the packet information (MAC header information, IP header information, transport header information, and application information), enables the data collector to detect network intrusions based in the different layers of the OSI model (see column 7, lines 18-24). Therefore, it would have been obvious to one ordinary skill in the art at the time the invention was made to use an operating system with network stack comprising protocol driver and a media access control driver because it would allow the operating system to interpret the information collected from the packets in order to analyze and detect network intrusions as suggested by **Vaidya**.

As per claim 2: the references as combined above disclose the claimed node of claim 1. **Farley et al** discloses at least one field comprises vulnerability status (enabled) (page 13, paragraph 155) and priority status (severity) (paragraphs160-161) that meets the recitation of at least one field comprises a field selected from the group consisting of an ENABLED field and a SEVERITY field.

As per claim 3: the references as combined above disclose the claimed node of claim 1. **Farley et al** further discloses wherein the node is operable to compile the text-file into a machine-readable signature-file and transmit the machine-readable signature-file to at least one other node of the network (see page 6, paragraphs 66-68 and page 8, paragraph 93) (generating raw event, organizing, correlating them and sending them to console which is interpreted as meeting the claimed limitation of compiling and transmitting).

As per claim 4: the references as combined above disclose the claimed node of claim 1. **Farley et al** further discloses the node operable to store a plurality of text-files, each respectively defining a network-exploit rule, in the database (see page 8, paragraphs 97-98 and fig. 2).

As per claim 5: the references as combined above disclose the claimed node of claim 2. **Farley et al** further discloses a machine readable signature-file database operable to store a plurality of machine-readable signature-files each generated from one of a respective plurality of text-files (see page 8, paragraphs 96-97), the management application operable to transmit a subset of the plurality of machine-readable signature-files to another node connected to the network (see page 6, paragraphs 67-68 and page 8, paragraph 93). **Farley et al** further discloses the database may include a database raw event classification that contains categories of different raw events (par.18) to be forwarded to specific node (paragraph 192).

.

. **As per claim 6**: the references as combined above disclose the claimed node of claim 5. **Farley et al** further discloses the database may include a database raw event classification that contains categories of different raw events (par.18) to be forwarded to specific node (paragraph 192); for example the database may also contains a list of raw events permitted to have priority status change and not priority permitted to have status change based on the vulnerability status value (vulnerable, not vulnerable, unknown (paragraph 155)) (see page 14, paragraphs 164, 166-167) (see also another example of lists generated with priority status allowed or disallowed (see page 15, paragraph 168) that meets the recitation of wherein the subset comprises all machine-readable signature-files of the plurality of machine-readable signature-files each generated from a respective text-file having an asserted ENABLED field value.

As per claim 7: the references as combined above disclose the claimed node of claim 5. **Farley et al** further discloses wherein management application is operable to accept a SEVERITY threshold from the input device and the subset of signatures comprises all machine-readable signature-files respectively generated from a text-file having a SEVERITY field value equal to or greater than the threshold (see pages 8-9 paragraphs 98-99 and page 15, paragraph 171).

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 8-20 are rejected under 35 U.S.C. 102(e) as being anticipated over US Patent Publication US 2002/0078381 to **Farley et al.**

As per claim 8: Farley et al discloses a method of distributing command and security updates in a network having an intrusion protection system, comprising: generating a text file (raw event or event log file) defining a network-exploit rule (see pages 6-7 paragraphs 76-77 and claim 9); specifying at least one field during generation of the text file such as historical frequency value, frequency value, or vulnerability status; each meets the recitation of at least one field selected from the group consisting of an enabled field value and a severity level field value during generation of the text file. As interpreted by Examiner, the vulnerability status (page 13, paragraph 155) may be either vulnerable or not or unknown that meets the recitation of enabled field; the historical frequency value may be allowed or disallowed and further contains a threshold (see page 15, paragraphs 168-171), that meets the recitation of enabled field and a severity level field value; the priority status values meets the recitation of severity level field (paragraphs160-161). **Farley et al** further discloses the raw events may be received as a file or being read in event log file (see claim 4 and page 19, paragraph 209. Although not using the same wording, it is apparent to one of ordinary skill in the art that **Farley et al** discloses the claimed limitation of claim 8. As interpreted by Examiner raw event comprises text generated during generation of the event as shown in (fig. 5B and 5C and paragraphs 77, 160-161 and 155) raw event is interpreted as being generated as a text file because **Farley et al** discloses each event is stored in an event storage area (claim 14), event is received in a file (claim 4).

As per claim 9: **Farley et al** discloses storing a plurality of text-files in a database, each text-file defining a network-exploit rule (see pages 8-9, paragraph 98).

As per claim 10: **Farley et al** discloses the database may include a database raw event classification that contains categories of different raw events (par.18) to be forwarded to specific node (paragraph 192) that meets the recitation of transmitting, by a management node of the network, a subset of the plurality of machine-readable signature-files to a node in the network .

As per claim 11: **Farley et al** discloses the database may include a database raw event classification that contains categories of different raw events (par.18) to be forwarded to specific node (paragraph 192); for example the database may also contains a list of raw events permitted to have priority status change and not priority permitted to have status change based on the vulnerability status value (vulnerable, not vulnerable, unknown (paragraph 155)) (see page 14, paragraphs 164, 166-167) (see also another example of lists generated with priority status allowed or disallowed (see page 15, paragraph 168) that meets the recitation of wherein the subset comprises all machine-readable signature-files of the plurality of machine-readable signature-files each generated from a respective text-file having an asserted ENABLED field value.

As per claim 12: the references as combined above disclose the claimed node of claim 5. **Farley et al** further discloses wherein management application is operable to accept a SEVERITY threshold from the input device and the subset of signatures comprises all machine-readable signature-files respectively generated from a text-file having a SEVERITY field value equal to or greater than the threshold (see pages 8-9 paragraphs 98-99 and page 15, paragraph 171).

As per claim 13: **Farley et al** discloses a computer-readable medium having stored thereon set of instructions to be executed, the set of instructions, when executed by a processor, cause the processor to perform a computer method of: (a reader) for reading input from an input device of the computer (paragraph 93); reading the raw event and creating raw event data objects that meets the recitation of compiling the input into a machine readable signature file comprising machine-readable logic representative of the network-exploit rule (see paragraph 93); also (see page 6, paragraphs 66-68 and page 8, paragraph 93) (generating raw event, organizing, correlating them and sending them to console which is also interpreted as meeting the claimed limitation of compiling) and vulnerability status (enabled) (page 13, paragraph 155) and priority status (severity) (paragraph 161) that meets the recitation of a value of at least one field selected from the group consisting of an ENABLED field and a SEVERITY field. **Farley et al** discloses evaluating the machine readable signature file and determining the value of the at least one field of the machine readable signature file (see pages 8-9, paragraph 98 and page 14, paragraphs 161, 162, and 165). Another example is disclosed in paragraphs 168-171 with respect to evaluating and determining raw events based on frequency event types.

As per claim 14: **Farley et al** discloses comprising a set of instructions that, when executed by the processor, cause the processor to perform the computer method of specifying a SEVERITY threshold value (see paragraphs160-161 and 171).

As per claim 15: **Farley et al** discloses the database may include a database raw event classification that contains categories of different raw events (par.18) to be forwarded to specific node (paragraph 192) that meets the recitation of transmitting the machine-readable signature file to another node of the network upon determining the value of the SEVERITY field is greater than the threshold (see pages 8-9 paragraphs 98-99 and page 15, paragraph 171).

As per claim 16: **Farley et al** discloses generating a text file from the input the text file specifying the network-exploit rule, and the at least one field, the machine readable signature file compiled from the text file(see page 6, paragraphs 66-68 and page 8, paragraph 93)

As per claim 17: **Farley et al** discloses the database may include a database raw event classification that contains categories of different raw events (par.18) to be forwarded to specific node (paragraph 192); for example the database may also contains a list of raw events permitted to have priority status change and not priority permitted to have status change based on the vulnerability status value (vulnerable, not vulnerable, unknown (paragraph 155)) (see page 14, paragraphs 164, 166-167) (see also another example of lists generated with priority status allowed or disallowed (see page 15, paragraph 168) that meets the recitation of wherein the subset comprises all machine-readable signature-files of the plurality of machine-readable signature-files each generated from a respective text-file having an asserted ENABLED field value (see also paragraph 192).

As per claim 18: **Farley et al** discloses wherein the intrusion protection system management application is further operable to determine, based at least in part on the at least one field, ones of a plurality of other nodes to which the network-exploit rule is to be distributed (see paragraph 192).

As per claim 19: **Farley et al** discloses vulnerability status (enabled) (page 13, paragraph 155) and priority status (severity) (paragraph 161) and further discloses whether adjusting priority value should be performed based on vulnerability status information (see paragraphs 164, 166, and 167) that meets the recitation of wherein the ENABLED field value specifies whether the network-exploit rule is enabled for evaluation by an intrusion protection system, and wherein the SEVERITY level field value specifies a severity level of the network-exploit rule.

As per claim 20: **Farley et al** discloses distributing the network-exploit rule and the at least one field to a plurality of nodes (see paragraph 45) and determining by an intrusion protection system of each of the plurality of nodes, based at least in part on the at least one field, whether to evaluate the network-exploit rule in protecting the intrusion protection system's respective node (see paragraphs 118-119 and paragraph 167).

Conclusion

5. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Non-Patent Literature: "State Transition Analysis: A Rule-Based Intrusion Detection Approach" by Koral et al discloses fact-base and rule-base storing information such as action and event types for network intrusion detection as text file comprising fields.

Patents: US Patent 7,085,936 Moran 7,116,663 Liao.

5.1 Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carl Colin whose telephone number is 571-272-3862. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser G. Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

CC

Carl Colin
Patent Examiner
May 10, 2007

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER